Cisco Intercloud Services

Telstra User Guide

2.2

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Copyright © 2014-2015 Cisco Systems, Inc. and/or its affiliates. All Rights Reserved.

The information contained in this document is proprietary and confidential to Cisco Systems, Inc. (“Cisco”) and/or its affiliates, and is furnished in confidence to you under the Confidentiality terms of the applicable agreement between you and Cisco, with the understanding that it will not, without the express written permission of Cisco, be used or disclosed for other than for the purposes set forth in that agreement.

Information about Cisco Services and technology may be subject to export controls under the laws of the United States and other countries. You and Cisco shall comply with such laws and you agree not to knowingly export, re-export or transfer such information without first obtaining any required United States or any other applicable authorizes or licenses.

The trademarks, logos and service marks ("Marks") displayed in this document are the property of Cisco or third parties. Users are not permitted to use these Marks without the prior written consent of Cisco or such third party which may own the Mark. "Cisco" is a registered trademark of Cisco and/or its affiliates.

The design in this document may contain or reference software from the open source community, including OpenStack® technology, that must be licensed under the specific license terms applicable to such software. http://www.apache.org/licenses/LICENSE-2.0.

Table of Contents

Document History 6
1. Preface 7
About This Guide 7
Audience 7
2. Cisco Intercloud Services Overview 7
Terminology 7
Summary of Available Services 8
Cisco Intercloud Services Interfaces 8
The Cisco Intercloud Services Console 8
Horizon 8
Accessing the Cisco Intercloud Services Platform 9
Choosing a Region 9
Other Ways to Access CIS 10
3. Starting with a Project 10
Create a Project 10
Create Multiple Projects 10
4. Network Management 11
View Your Network Elements and Routers 11
Create a Private Network and Attach a Router to Make the Subnet Externally Accessible 11
Create a Network 11
Create a Subnet 11
Create a Router 12
Telstra Next IP 13
Create Networks and Subnets in Your Project 13
Create a Router 13
Create Router Interfaces 13
Request Telstra Next IP 14
Configure Your Project Router 15
Modify Security Groups as Appropriate 15
Create or Modify Your Project Firewall 16
Create a Virtual Private Network 16
Firewall as a Service 16
Create a Firewall Rule 17

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Create a Firewall Policy 17
Create a Firewall and Add a Policy 17
5. Cryptographic Key Pairs for Security 18
Generate a Key Pair from Horizon 18
Import a Key Pair 19
6. Provision a Virtual Machine Instance 20
Create Your First VM Instance 20
Windows VM Key Management Service Activation 22
Activating Non-CIS Windows Images 22
Troubleshooting 23
Affinity and Anti-Affinity 23
Security Groups 23
Using the Default Security Rule 24
Adding a Rule for Security Groups 24
Remote Desktop Protocol for Windows Images 24
Floating IP Addresses 25
Access Your First VM Instance 25
SSH from an External Terminal (Linux) 25
Access a Linux VM via the Instance Console 26
Access a Windows VM via the Instance Console 26
DNS Registration 27
Managing Volumes before Terminating a VM Instance 27
Terminate a VM Instance 27
7. Load Balancing as a Service 28
Create a Load Balancer 28
Create a Load Balancer Pool 29
Assign a Virtual IP Address to the Load Balancer 29
Add VM Members to the Pool 30
Add Health-Check Monitors to the Load Balancer 31
Attach a Floating IP Address to the Load Balancer 31
Test the Load Balancer 32
8. Images and Snapshots 33
Images 33
Launch a VM from an Existing Image 33

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Create an Image 33
Snapshots 34
Create an Instance Snapshot 34
Create a Volume Snapshot 34
Create a Volume from a Snapshot 35
9. Storage for your VM: Volume and Object 35
Create Volume Storage and Attach / Mount it to Your VM 35
Create Volume Storage 35
Attach a Volume to a VM (Linux) 36
Attach a Volume to a VM (Windows) 36
Detach a Volume from a VM 37
Object Storage 37
Overview 37
Create a Container 38
Upload an Object to a Container 38
Delete an Object 38
Delete a Container 39
10. Accessing CIS via OpenStack CLIs & REST APIs 39
Generate Your API Key 39
Download the OpenStack RC file 39
11. Glossary 40
12. Appendix: Resource Segregation 43
Creating a Filter Policy 43
Use the Nova Command-Line Tool 43
Use the REST API 43
Placing Instance on Different Computer Hosts 44
Use the Nova Command-Line Tool 44
Use the REST API 44
13. Appendix: CIS Instance Customization 45
Cloud-init and Cloudbase-init 45
Sample Customization Options 46

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Document History

Topic	Date of Change	Description
Create a Private Network and Attach a Router to Make the Subnet Externally Accessible > Create a Router (page 11) (2.1)	6/11/15	Added a note that they can only create one router per project.
Firewall as a Service (page 16) (2.1)	6/11/15	Removed any reference to the **Shared** check box from these subordinate topics: • **Create a Firewall Rule** (step 3f and the Note which referred to step 3f) • **Create a Firewall Policy** (step 3c) • **Create a Firewall and Add a Policy** (step 3d)
Chapter 7: Load Balancing as a Service (2.1)	6/15/15	Removed **Choosing a Region** topic.
Choosing a Region (page 9) (2.2)	6/19/15	Added as a sub-topic following the **Accessing the Cisco Intercloud Services Platform** topic.
Choosing a Region (page 9) (2.2)	6/22/15	Made the following changes: • Removed the first Note. • Cropped the screen shot to remove URL and bookmarks.
Choosing a Region (page 9) (2.2)	7/1/15	Made the following changes: • Updated text per Daniel's feedback. • Used screen shot provided by Daniel.
Choosing a Region (page 9) (2.2)	7/2/15	Made the following changes: • Used screen shot provided by Daniel, which shows the error message. • Re-arranged Note text since screen shot was of log in screen.
Choosing a Region (page 9) (2.2)	7/2/15	Made the following changes: • Per Darryl, put the text back to its original flow, with a screen shot of only the message • Include a log in screen shot.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

1. Preface

About This Guide

This guide is for users who want to learn how to create and manage projects using the Cisco Intercloud Services (CIS) platform. The information provided in this guide presumes you already have a CIS account.

Audience

This guide is primarily intended for users of the cloud, whose skill set can vary from beginners to advanced developers of cloud applications or system administrators managing IaaS.

2. Cisco Intercloud Services Overview

In some respects, CIS might work slightly differently than other cloud services that you have used. Review the relevant sections in this document before beginning your cloud development efforts.

Terminology

You need to become familiar with the following terms to understand the procedures in this guide. For a complete list of terms, refer to the Glossary on page 40.

- **OpenStack** - An open source cloud computing platform.
- **Project** - A virtual space or unit in the CIS cloud that can be assigned to a user or users. Each project is provided access to VM instances and is assigned a quota of virtual resources.
- **Tenant** - The entity that owns a project. A tenant can have more than one project.
- **Region/Data Center** - These terms are used interchangeably in Horizon and the CIS Console to refer to the data center that hosts the project account services.
- **Virtual Machine (VM), Server, or Instance** - In OpenStack, a VM is created by a user and is composed of a guest operating system, one or more CPUs (cores), storage, and network components. Also called a server or an instance.
- **InstanceType/Flavor** - Describes the configuration of the various virtual machine flavors (configurations) that are available to users. It includes parameters such as CPUs (cores), storage, and memory. When you launch an instance, the flavor that you specify determines the amount of RAM, disk space, and the number of virtual CPUs used.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Summary of Available Services

CIS offers the following services:

- **Virtual Compute** — Virtual servers (VM instances) with a choice of flavors (virtual CPU, RAM, and storage).
- **Virtual Storage** — Choice of volume storage and object storage services.
- **Virtual Network** — Provision your own network topologies with virtual routers, and public and private IP addresses.
- **Virtual Private Network (VPN)** connectivity
- Load Balancing as a Service (LBaaS)
- Heat Orchestration (Beta)

CIS platform capabilities include:

- **Security Groups** — Ability to apply security rules and policies that govern access to VMs.
- **Firewall as a Service** – Ability to apply security rules and policies that govern access to project networks via FWaaS on the router.
- **Programming Support** — Ability to access cloud services using:
    - OpenStack Command line interface (CLI) access to CIS.
    - OpenStack Representational State Transfer (REST) API access to CIS.

Cisco Intercloud Services Interfaces

A web browser is your access to all CIS user interfaces. Mozilla Firefox is recommended.

Note: The CIS user interfaces support the current release and one prior release of Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, and Apple Safari on a rolling basis.

The Cisco Intercloud Services Console

From the Cisco Intercloud Services Console you can:

- Access CIS documentation (via the Support link).
- View quota limits for various network components.
- View reports on project usage for time periods that you specify.
- Access the Telstra Cloud Services Portal to manage users, or sign up to connect your CIS project to your enterprise via Telstra Next IP.

Horizon

Horizon allows you to implement and manage CIS functionality including:

- Networks, network topology, routers, firewall-as-a service (FwaaS), and load balancer-as-a-service (LBaaS)

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

- Key pairs
- VMs
- Security groups
- Volumes
- Images
- Snapshots

Accessing the Cisco Intercloud Services Platform

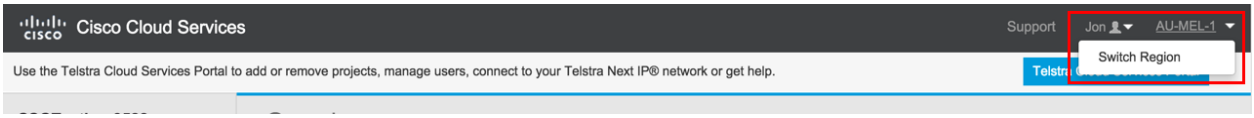
To access the Cisco Intercloud Services Console:

1. Log in to the Telstra Cloud Services Portal: https://mycloud.telstra.com.
2. Click the **Cisco console** tab.
3. The first time you log in, you are prompted to agree to the Acceptable Use Policy (AUP). Read the AUP, and, if you agree to the terms and conditions of the AUP, accept it. The CIS Console opens. Use of CIS indicates that you accept the terms and conditions of the AUP.

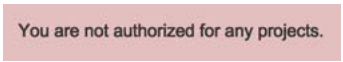
Choosing a Region

When you log in, you can choose the region containing the project you want to work on by clicking the button for that region in the login window.

After logging in, you can dynamically switch regions to access a project in another region. Click the down arrow next to the region name in the black navigation bar, top right, and select **Switch Region.**


Cisco Cloud Services
Support
Jon
AU-MEL-1
Switch Region
Use the Telstra Cloud Services Portal to add or remove projects, manage users, connect to your Telstra Next IP® network or get help.

Note: If you attempt to access a region in which you do not have a project, you will get an error message.



Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Other Ways to Access CIS

There are other ways to access CIS that are detailed in this guide:

- Command Line Interface (CLI) – Refer to Accessing CIS via OpenStack CLIs & REST APIs on page 39.
- Application Programming Interface (API) – Refer to Accessing CIS via OpenStack CLIs & REST APIs on page 39.

3. Starting with a Project

You can start using CIS after you are added to your first project. You'll receive a welcome email with next steps.

Create a Project

Project creation is managed via the Telstra Cloud Services Portal.

To create a project:

1. Log into the Telstra CIS Portal: https://mycloud.telstra.com.
2. Click the **Cisco Intercloud Services** tab.
3. Click **Add Project**.
4. Follow the prompts for creating a project.

Create Multiple Projects

You can create more than one project if you need to. However there are times when you'll want to keep expanding an existing project instead of creating a new one.

For example, VMs that are going to communicate with each other should be on the same private network range in the same project. As a rule of thumb, don't create situations in which projects have to talk to each other.

However, if the VMs are not going to communicate with each other and are going to be isolated, you can just put one or a few VMs in each project.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

4. Network Management

All virtual machines (VMs) must be attached to a network in order to be functional. When a new project is created, by default there is no network associated with the project. Therefore the first thing you have to do is provision a network.

Cisco Intercloud Services (CIS) offers a comprehensive set of network services that allows you to:

- Define and configure your own private virtual networks using routers and gateways.
- Allocate and manage public floating IP addresses that allow your users to access your VMs via the Internet.

View Your Network Elements and Routers

To view a screen with layout of your network elements and routers, click Network > Network Topology from the Horizon left panel.

Create a Private Network and Attach a Router to Make the Subnet Externally Accessible

Create a Network

You can create your own private network. For example, you could create a private network called **my-first-network** and assign it an RFC 1918 address space of 192.168.1.0/24.

Note: The address spaces used in this document are for example purposes only.

1. Click Network > Networks in the Horizon left panel.
2. Click Create Network.
3. In the Create Network dialog, enter “my-first-network” in the Network Name field.

Create a Subnet

1. Click Next.
2. In the Create Subnet dialog, enter “my-first-private-subnet” in the Subnet Name field.
3. Enter 192.168.1.0/24 in the Network Address field.
4. The first address of this range, 192.168.1.1, is the default gateway. You will use the default gateway so leave the Gateway IP field empty.
5. Click Next.
6. You can specify additional attributes for the subnet in Subnet Details. Ensure that the Enable DHCP check box is selected. All other parameters in this screen are optional.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

7. Click Create to complete private network provisioning. You'll see that 'my-first-private-subnet' was created and appears in the list of networks.
8. Click Network Topology to see that your private network was added to the network topology view.

Create a Router

Create a virtual router to route traffic between a private network and another network, for example a public network for Internet access.

Note: You can only create one router per project.

To create a router:

1. Click Network > Routers from the Horizon left panel.
2. Click Create Router.
3. Enter a name for the router in the Router Name field, for example "My-Test-Router".
4. Click Create Router.
5. The router appears in the Routers list.
6. To set up a gateway for the router, click Set Gateway.
7. From the drop-down list, set the External Network to a public-floating address. Typically, **public-floating-601** is available.
8. Click Set Gateway to attach the router to the public network.
9. Click Network Topology to see that the router was created and connected to the public floating IP network.
10. To connect the router to the private network you created earlier, hover the mouse cursor over the icon for the router in the Network Topology screen, then click View Router Details. (Alternatively you could click the router name in the Horizon Routers screen.)

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

11. In the screen that appears, click Add Interface.
12. In the Subnet field select the “my-first-private-subnet” subnet that was created earlier.
13. Click Add Interface.
14. To verify that the router was connected successfully, click Network Topology. Ensure that the private network displays in orange and that the router displays as a small box that connects the public network to the private network.

Telstra Next IP

If you have the Telstra Next IP service you can connect your CIS project’s deployed OpenStack networks to your enterprise via Telstra Next IP.

Create Networks and Subnets in Your Project

The first step is to create networks and subnets in your project if you haven’t done so already. (You can add additional networks and subnets at a later date and make an additional request for Telstra Next IP as described below.)

Create a Router

If you haven’t already done so, create an OpenStack Neutron router for L3 routing capabilities via Horizon, the OpenStack CLIs, or the OpenStack APIs.

Note: You can only create one router per project.

Create Router Interfaces

Create an interface on the project’s router for any networks which need L3 routing capacities, either between other CIS networks or your enterprise networks reachable via Telstra Next IP.

Any networks that are connected to the router will be advertised (i.e., L3 routing destinations) to your enterprise.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

You can add an internal network interface to your router via Horizon (Network > Routers > Add Interface) or via the OpenStack CLI:

neutron router-interface-add [-h] [--request-format {json,xml}] <*router-id*> <*interface*>

Where:

router-id is the ID of the previously created router

interface is in the format of:

<*subnet ID*>

subnet=<*subnet ID*> (optional – just listing the subnet ID is permitted)

port=<*port ID*>

A subnet or a port must be specified.

Optional arguments:

-h, --help show this help message and exit

--request-format {json,xml}

Example adding an interface to the router "my-router" with the subnet ID of xxxxxxx-xxxxxxx:

neutron router-interface-add my-router xxxxxxx-xxxxxxx

To list the interfaces attached to the router execute the following command with the router's name or ID as the only argument:

neutron router-port-list <*router name* | *router ID*>

Example:

neutron router-port-list my-router

Request Telstra Next IP

Click Telstra Cloud Services Portal in the CIS Console, navigate to the Cloud Direct Connect page, and follow the Telstra instructions for implementing Telstra Next IP in your project.

You need to submit the following information:

- NRFNN (optional)
- An eBGP Interconnect Subnet /29. If you have projects in multiple CIS regions, an Interconnect Subnet is required for each region.
- A Transition Network Subnet /29 for your project.

When Telstra Next IP is provisioned in your CIS project, it displays as a new provider network icon in the Horizon Network Topology view. It will be attached to your project router. If you did not have a Neutron router provisioned in your project, a Neutron router will be provisioned for you. However you will then have to create an interface on your project's router for each network that you want to connect to Telstra Next IP.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

IMPORTANT: Do ***not*** add any VMs or any other network components to the dedicated Telstra Next IP provider network.

All OpenStack networks that existed in the project and were connected to the Neutron router when Telstra Next IP was provisioned will be connected to your enterprise via Telstra Next IP when you configure your project router.

Subsequent OpenStack networks added to your project will not be connected to Telstra Next IP unless you create router interfaces for them and then submit another request for Telstra Next IP from the Cloud Direct Connect page. When the new request is implemented, all existing networks that are connected to the Neutron router in your CIS project will have Telstra Next IP connectivity.

Configure Your Project Router

After your Telstra Next IP network is provisioned in your project you must configure your project's router with:

- The CIDR addresses of the destination subnets that you want to reach in your enterprise, and
- The next hop IP address needed to reach those networks.

Configuring static routes via Horizon is not currently possible, so you must do this via the OpenStack CLIs or APIs.

This example configures a project router with the CIDR addresses of three destination subnets in an enterprise and the IP address of the next hop router. The IP address of the next hop router is the same for all destination subnets.

```
# neutron router-update  <project-router-name>  --routes type=dict  list=true
  destination=xxx.xx.xx.0/30,nexthop=xxx.xxx.xxx.xxx
  destination=xxx.xxx.x.0/30,nexthop=xxx.xxx.xxx.xxx
  destination=xxx.xxx.xxx.0/24,nexthop=xxx.xxx.xxx.xxx
```

The destination subnets shown above represent subnets in your enterprise that are reachable via the Telstra Next IP service.

The nexthop IP address is the last host address in the transition subnet that you supplied when you submitted your request for Telstra Next IP®.

To see the static routes that the router-update command configured in the project's Neutron router, execute the
neutron router-show command:

```
# neutron router-show <project-router-name>
```

Modify Security Groups as Appropriate

You may need to modify the security groups in your project to permit various types of traffic between your enterprise and your VMs. For example, if you have a web server on a VM in your project receiving requests from clients in your enterprise, you will have to modify the VM's security group to allow TCP ingress on port 80.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

You can also restrict the source of web requests to a specific remote subnet or a single IP address. Likewise you can restrict outgoing traffic from your VMs. Cisco strongly recommends restricting ingress and egress traffic to/from your VMs to only allow required traffic.

For more information refer to Security Groups on page 21.

Create or Modify Your Project Firewall

You can also create/modify your project's perimeter firewall capabilities to allow specific types of traffic to/from your enterprise, and you can limit the source/destination of that traffic to specific local or remote subnets/ports. Cisco strongly recommends restricting ingress and egress traffic to/from your project to only allow required traffic.

Create a Virtual Private Network

You can create a virtual private network (VPN) that connects your CIS project to one of your data centers using the Cisco Intercloud Services Router 1000V (CSR 1000V) virtual router.

You can access to the Cisco Intercloud Services Router 1000V Policy-based VPN Tunnel Guide at: https://www.telstra.com.au/content/dam/tcom/business-enterprise/cloud-services/pdf/cisco-router1000v-vpntunnel-guide.pdf

Firewall as a Service

You can implement OpenStack Firewall as a Service (FWaaS) functionality in your project to add perimeter security for your project via your router. Although it's technically possible to have more than one router in a CIS project, overwhelmingly the typical use case is one router per project.

While OpenStack security groups with their security rules are designed to add security to VMs, OpenStack FWaaS is designed to add security to the CIS project periphery at the router.

Note: If your Windows® VMs are going to access the Remote Desktop Protocol (RDP) over the Internet, then RDP port 3384 must be open in your project's FWaaS.

The steps to set up FWaaS for a project are:

- Create one or more firewall rules.
- Create one or more firewall policies.
    - Add one or more rules to each policy.
- Create a firewall.
    - Add a policy to the firewall.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Create a Firewall Rule

1. In Horizon, navigate to Network > Firewalls.
2. Click Firewall Rules.
3. Click Add Rule:
    a. Type a name for the firewall rule in the Name field.
    b. Select a protocol from the Protocol drop-down.
    c. Select Allow or Deny in the Action drop-down.
    d. Specify source and/or destination IP addresses/subnets.
    e. Specify source and/or destination ports/port ranges.

Create a Firewall Policy

1. In Horizon, navigate to Network > Firewalls.
2. Click Firewall Policies.
3. Click Add Policy:
    a. Type a name for the firewall policy in the Name field.
    b. Optionally type a description for the policy in the Description field.
    c. Click the Audited check box if you want to audit changes to underlying rules or policies
    d. Click Rules.
    e. Click the plus sign for each of the rules you wish to add to this policy.
    f. Click Add. In a few moments the new policy will appear in the Firewall Policies screen.

Create a Firewall and Add a Policy

1. In Horizon, navigate to Network > Firewalls.
2. Click Firewalls.
3. Click Create Firewall:
    a. Type a name for the firewall in the Name field.
    b. Optionally type a description of the firewall in the Description field.
    c. Select the policy for this firewall in the Policy drop-down.
    WARNING: If you deselect Admin State the firewall will be turned off.
    d. Click Add. The new firewall appears in the Firewalls screen.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

5. Cryptographic Key Pairs for Security

Create a key pair before creating a Linux VM (CIS Windows images do not use keypairs.)

Cisco strongly recommends using cryptographic keys to add security to your VMs. You can use a cryptographic key pair that you have used previously for secure shell (SSH), or you can create a new key pair using the CIS user interface. Refer to Generate a Key Pair from Horizon on page 18.

Key pairs are SSH credentials that are injected into instances when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file). The public key is associated with the image for the instance. The private key is stored on your computer.

You can create multiple keys for an instance. For example, you might want to have a set of keys to use in multiple locations. Alternately, you can use one key pair for a set of instances.

IMPORTANT: Protect and use the key as you would any SSH private key.

Each keypair has two parts: the public key and the private key.

- The public key is maintained and supplied by the OpenStack identity management system. When an instance is generated, the public key is automatically injected into the instance by CIS. You need the private key to authenticate the SSH session.
- The private key is stored on your computer as a .pem file.

Generate a Key Pair from Horizon

To generate a key pair for an instance from Horizon:

1. Click Compute > Access & Security.
2. Click Key Pairs.
3. Click Create Key Pair.
4. In the Keypair Name field, enter a name like **my-first-keypair**. Lower case is recommended to avoid potential system-level case conversion incompatibilities.
5. Click Create Keypair.
6. In the dialog that appears, select Save File, then click OK to download the .pem file.
7. You can use this .pem as part of SSH access. This is the private key.

   Note: The .pem file that was downloaded onto your computer must have rw------- permissions to SSH into the VM. If not, change the permissions:

   $ ls -la my-first-keypair.pem

   $ rwx------

   $ chmod 600 my-first-keypair.pem

   $ ls -la my-first-keypair.pem

   $ rw-------

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Import a Key Pair

You can import a key pair into CIS. For example, you might have an SSH key pair that you have generated and used previously that you want to keep using.

To import a key pair:

1. Click Compute > Access & Security in the Horizon left panel.
2. Click the Key Pairs tab.
3. Click Import Key Pair.
4. Type the key pair name in the Key Pair Name field.
5. Copy the contents of your public key and paste that text into the Public Key textbox.
6. Click Import Key Pair.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

6. Provision a Virtual Machine Instance

Create Your First VM Instance

1. Before you create your first VM instance, ensure that you have the following:
   a. You have a valid network/subnet created. The VM creation process needs a network name.

      IMPORTANT: If you have not created a network, cancel out of this process of creating a VM and provision a network / subnet. If the VM has to be publicly accessible, provision a router and associate the router to the Gateway.

   b. You have a valid SSH key pair generated (Linux only).

      WARNING: If you haven't created a key pair via CIS and you don't have an available valid SSH key pair that you have previously imported into CIS, cancel out of this process of creating a VM. Go to Generate a Key Pair from Horizon on page 18 or Import a Key Pair on page 19. When you have created or imported an SSH key pair, return to this section and continue with the next step.
2. Click Compute > Instances.
3. Click Launch Instance.

   Enter the following Instance Details:

   Availability Zone: Note: Availability zones may vary depending on the data center.

   Instance Name: Type the name for your instance.

   Flavor: GP.Small (availability may vary depending on the data center)

   Number of instances: You can provision as much as allowed by the project quota. You can see your project quotas on the right side of the screen in the Flavor Details and Project Limits sections. Enter the number 1

   Instance Boot Source: You can point to any source. First-time users select Boot from Image

   Image Name: Select an image from the drop-down list.

   Note: Projects can deploy multiple instances using the same source image.
4. Click the Access & Security tab. This step is for Linux only. For Windows images skip to step 7 "Click the Networking tab."
5. In the Import Key Pair dialog, select an available key pair. This step is for Linux only – for Windows images skip to step 7 "Click the Networking tab."
6. Linux: If you haven't created a key pair via CIS and you don't have an available SSH key pair that you have previously imported into CIS, cancel out of this process of creating a VM and go to Generate a Key Pair from Horizon on page 18 or Import a Key Pair on page 19. When you have created or imported an SSH key pair, return to the process of creating a VM and select a key pair in this step.
7. Click the Networking tab.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

8. Click a network "+" button in the Available Networks field. The selected network moves to the Selected Networks field. If you are following the tutorial click the plus button for my-first-network.
9. Click the Post-Creation tab.

   Although there are many possible post-creation scripts for both Linux and Windows, that discussion is out of scope for this procedure.

   Note: Refer to Appendix 14: CIS Instance Customization on page 40 for sample post-creation scripts.

   This section only describes what is necessary to log into a VM running a Linux OS via the Instance Console. Windows instances are accessible from the Instance Console without a post-configuration script. Windows instance names cannot be longer than 15 characters.

   LINUX:

   For access to your instance using the Instance Console, set up an initial password which you will be prompted to change upon first login. For RHEL use the login name root, for Ubuntu use the login name ubuntu.

   Copy and paste the sample script below into the Post-Creation Customization Script text box including #cloud-config. Replace the password placeholder with an appropriate temporary password.

   #cloud-config

   password: *my-initial-password*
10. Click Launch.

    CIS provisions your new VM and the new VM appears in the Instances screen. Wait until provisioning is complete before trying to inspect or use the VM. The VM is attached to your private network, and the VM uses the image and SSH key pair that you selected during the creation process.
11. To manage/control an instance, select an action from the instance's More button. You can associate or disassociate a floating IP address, edit the instance or its security groups, navigate to the instance console, view the instance's log, or you can pause, suspend, soft reboot, hard reboot, shut off, or terminate the instance.

    WARNING: If you want attached volumes and their data to persist, the volumes **MUST** be detached before terminating the VM. ***Otherwise the attached volumes and their data will be destroyed.*** This does not apply to ephemeral data and the root boot disk. When an instance is terminated, the instance's ephemeral data are destroyed and all data in the instance's root boot disk are destroyed. Refer to Managing Volumes before Terminating a VM Instance on page 27.
12. Click Network > Network Topology to see that your instance has been provisioned and is attached to your private subnet.

    Tip: You can click elements in the Networking Topology screen to get more information about them and jump to relevant detail and configuration screens.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Windows VM Key Management Service Activation

CIS-provided Windows images have been configured to automatically activate using the key management service (KMS) provided by CIS. A public DNS record has been created for these KMS servers. If you're using a CIS-provided Windows images and your VMs have Internet access you do not need to do anything else, you can skip this section.

However, if you created a Windows image (refer to Create an Image on page 33) you will have to activate Windows.

CIS provides a key management solution for activating Windows Server operating systems. The CIS Microsoft Windows 2012 R2 Server license supports activation of the following operating systems:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2012 R2 Standard

Activating Non-CIS Windows Images

All Non-CIS Windows images (launched from an image that you created) need to be activated using the CIS-provided KMS.

Prerequisites:

- Every Windows VM requires at least one network adapter to establish connectivity with the host kms.telstra.cloud.cisco.com
- Each Windows instance must have Internet access to be able to obtain activation.
- KMS activations are valid for 180 days—the *activation validity interval.* To remain activated, KMS client computers must renew their activation by connecting to the KMS host at least once every 180 days. If a VM is in an isolated network and unable to contact the KMS host, activation will fail.

Verify the KMS Client Product Key

Consult the following table to see if the Windows version you are activating has the correct KMS client product key.

Operating System Edition	**KMS Client Product Key**
Windows Server 2008 R2 Standard	YC6KT-GKW9T-YTKYR-T4X34-R7VHC
Windows Server 2008 R2 Enterprise	489J6-VHDMP-X63PK-3K798-CPX3Y
Windows Server 2012 R2 Standard	D2N9P-3P6X9-2R39C-7RTCD-MDVJX

If you don't have the correct client product key you can change it using the following steps:

1. Click the start button, right-click the command prompt icon, and select "Run as Administrator".
2. Enter this command using the correct KMS client product key: slmgr.vbs /ipk <*KMSClientProductKey*>
3. To verify that the key is set, execute: slmgr.vbs /dlv

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Manually Activating Windows

When you have the correct KMS client product key, manually activate the KMS client:

1. Click the start button, right-click the command prompt icon, and select “Run as Administrator”.
2. Enter this command to set the activation server:

   slmgr.vbs /skms “kms.telstra.cloud.cisco.com:1688”
3. Enter this command to activate Windows:

   slmgr.vbs /ato

Troubleshooting

Error: A problem occurred when Windows tried to activate. Error Code 0xC004F074

- This error is received when Windows cannot reach the KMS server. Make sure the instance has Internet connectivity.
- Verify that the DNS settings are correct and point to or forward to a publicly available DNS server.
- Verify that the correct time zone and time are set on the Windows instance. A time difference of more than 4 hours with the KMS server(s) will prevent successful activation.
- To verify that the appropriate KMS product client key is set, execute the following command from an administrative prompt and check the results:

  slmgr.vbs /dlv

  If the results show: Error: product key not found, then the KMS key is not configured. Look up the KMS key from the table of client product keys in the Verify the KMS Client Product Key section on page 22 and issue the following command from an administrative command prompt:

  slmgr.vbs /ipk <*KMSClientProductKey*>

Affinity and Anti-Affinity

It’s possible to create a VM on the same host as another VM (affinity) or on a different host (anti-affinity) via OpenStack CLI or API commands. At this time affinity and anti-affinity can’t be specified via Horizon. For more information, refer to the section in the Resource Segregation Appendix on page 41.

Security Groups

Security Groups control the network traffic associated with each instance. Each instance can be configured by rules to allow specific types of inbound and/or outbound traffic.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Using the Default Security Rule

The default security rule permits:

- TCP ingress for SSH on port 22 from any remote network.
- ICMP ingress on all ports from any remote network.
- To allow other types of inbound traffic, you must explicitly open a port associated with the type of traffic you want to allow. For example, if your project has a web server, open port 80 for TCP ingress. You can optionally restrict the origin of web requests coming in on port 80 to a specific remote subnet or the IP address of a specific machine.

Adding a Rule for Security Groups

Rules define which traffic is allowed to instances assigned to the security group.

To add a rule to a security group:

1. Click Compute > Access & Security > Security Groups.
2. Click Manage Rules for the security group to which you want to add/remove a rule, or to create a new security group click Create Security Group.
3. To add a rule click Add Rule. The Add Rule dialog appears.
4. From the Rule drop-down list, select the protocol for the rule.
5. From the Direction drop-down list, select either Ingress or Egress. Typically rules focus on ingress.
6. From the Open Port drop-down, select Port or Port Range. For TCP and UDP rules, you can open either a single port or a range of ports.
    a. Select Port for a specific port, such as Port 80 for HTTP.
    b. Select Port Range to specify both the starting and ending ports for the range. For ICMP rules, instead specify an ICMP type, and code in the spaces provided.
7. From the Remote drop-down list, specify the traffic source. Select CIDR or Security Group.
8. If you select Classless Inter-domain Routing (CIDR), CIS displays a CIDR field. Enter a CIDR address.
9. If you select a Security Group, you can choose the default security group or a security group that has already been created. Selecting a security group as the source allows any instance in that security group to access to any other instance according to this rule.
10. Click Add.

Remote Desktop Protocol for Windows Images

The Windows images provided in the image catalog have Remote Desktop Protocol (RDP) port 3389 open by default. However, you will need to open RDP port 3389 in your Windows VMs' security groups to allow the appropriate traffic. If you created your own Windows image, you will have to open RDP port 3389 in your Windows firewall as well.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

If you're going to access RDP over the Internet then you will also need to open RDP port 3389 in the project's perimeter via Firewall-as-a-Service.

Floating IP Addresses

Floating IP addresses allow you to assign a public-accessible IP address to a private VM that's located on a private subnet. Floating IP addresses are not limited to VMs. Floating IP addresses can also be mapped to load balancers and other network resources.

A floating IP address and a private IP address can be used at the same time on a single network interface. For example, the private IP address is likely to be used for accessing the VM by other VMs in the private network. The floating IP address is likely to be used for accessing the VM from the Internet.

Note: Before associating a floating IP address with a VM or other network resource, a router must front the private subnet. In other words, the VM or other network resource must be reachable via a router.

A floating IP address can be reassigned from a VM or other network resource to a different VM or other network resource.

Floating IP addresses are allocated from a shared pool of IP addresses. There is currently no way to reserve a specific IP address.

To create a floating IP address and associate it with a private VM:

1. Click Compute > Access & Security.
2. Click the Floating IPs tab.
3. Click Allocate IP to Project.
4. In the Allocate Floating IP dialog click Allocate IP. After a few moments a new IP address appears.
5. Click Associate from the Actions column for the new IP address.
6. In the Manage Floating IP Associations dialog, select the private IP address of the private VM from the Port to be Associated drop-down.
7. Click Associate. The VM is now associated with a public IP address, and the VM is accessible from both private and public networks.

   Note: This may take a few minutes to activate. Refresh the Instances screen in Horizon every minute or so. When the floating IP address appears under the VM's IP address the association has been activated.

Access Your First VM Instance

SSH from an External Terminal (Linux)

Your VM is up and running. You can ping or SSH into your VM via the floating IP address that you associated with the VM.

1. Open a terminal window on your local machine.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

2. SSH into your VM via the VM's floating IP address:

   $ ssh -i <*path/to/your/local/private/key*> root@<*floating IP address*>

   Notes:

   Depending on your version of Linux, you may need to use a different login besides "root", for example "ubuntu".

   To find the floating IP address that you associated with the VM, in Horizon click Compute > Access & Security, then click the Floating IPs tab.

   Your SSH session may prompt you for your Unix password. This is your password that you configured in the Post-Creation script. You may be prompted to change your password.

Access a Linux VM via the Instance Console

1. Click an instance link. There are many ways to click an instance link. For example, you could click Compute > Instances in the Horizon left panel and then click an instance in the Instance Name column.
2. Click the Console tab.
3. You may need to wait a couple of minutes the first time the Console initializes itself and displays the "login:" prompt, however it's typically faster to click the gray status bar and then press Enter to give focus to the console.
4. At the Login prompt enter the appropriate login name for your Linux distribution. For example, **root** for RHEL, **ubuntu** for Ubuntu, and **centos** for Centos.

   Note: If you have accessed this instance from a terminal via SSH, you may have changed this password. If so, going forward you must use this new password when you log into this Instance Console.
5. If you are still using the password from the Post-Creation script (for example you haven't changed the original password via SSH), change the original password now.
   a. Existing password: <***Enter your password from the Post-Creation script (refer to page* 21)**>.
   b. New password: <***enter your new password***>
   c. Retype new password: <***reenter your new password***>

Access a Windows VM via the Instance Console

1. Click an instance link. There are many ways to click an instance link. For example, you could click Instances in the Horizon left panel and then click an instance in the Instance Name column.
2. Click the Console tab.
3. You may need to wait a couple of minutes the first time the Console initializes itself.
4. You may need to click the gray status bar to give focus to the console.
5. The Windows image will take approximately 3-8 minutes to boot up. Click once on the screen if the installation process seems to hang on "Please wait for the Local Session Manager.."

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

6. You will be prompted to create a password. This will be your Windows Administrator password for this Windows instance. As mentioned earlier, you may have to click on the grey bar and press Enter in order for the password fields to accept input, and you may also have to wait for a minute before it is ready.

DNS Registration

CIS does not automatically assign a fully-qualified domain name (FQDN) for newly-created VMs.

CIS does not offer domain name hosting or registration services for non-Cisco domains at this time. For non-Cisco domains, use the normal procedures for assigning a domain name with your DNS registration or hosting service.

Managing Volumes before Terminating a VM Instance

WARNING: If you want attached volumes and their data to persist, the volumes **MUST** be detached before terminating the VM. ***Otherwise the attached volumes and their data will be destroyed.*** This does not apply to ephemeral data and the root boot disk. When an instance is terminated, the instance's ephemeral data are destroyed and all data in the instance's root boot disk are destroyed.

Before terminating a VM:

1. Carefully document the name and ID of each attached volume that you want to persist. If you are using Horizon the name will be sufficient, if you are using cinder you will also need the volume ID.
2. Detach each volume from the targeted VM one by one. For information about detaching a volume from a VM, refer to Detach a Volume from a VM on page 33.
3. Attach each volume to a new VM and verify that the volumes and their data are intact.
4. When you are certain that all the volumes you want to persist are detached and safely stored/verified/reattached to another instance, terminate the targeted VM as discussed below.

Terminate a VM Instance

WARNING: If you want attached volumes and their data to persist, the volumes **MUST** be detached before terminating the VM. ***Otherwise the attached volumes and their data will be destroyed.*** This does not apply to ephemeral data and the root boot disk. When an instance is terminated, the instance's ephemeral data are destroyed and all data in the instance's root boot disk are destroyed. Refer to Managing Volumes before Terminating a VM Instance on page 27.

1. Click Compute > Instances in the Horizon left panel.
2. Attached volumes will be destroyed in the next step. Be certain that you don't have any volumes that you want to persist attached to the instance targeted for termination. If you wish to save any volumes you must do so before proceeding. Refer the instructions in the Managing Volumes before Terminating a VM Instance section on page.
3. When you are sure that you don't have any attached volumes that you wish to save, click More in the target instance's Actions column. In the drop-down, click Terminate Instance.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

4. In the Confirm Terminate Instance dialog, click Terminate Instance if you are certain that you want to terminate the selected instance.

7. Load Balancing as a Service

Note: Load balancing does not display on the Horizon Network Topology screen.

A load balancer is a logical device that belongs to a cloud account. It is used to distribute workloads among multiple back-end systems or services based on the criteria defined as part of its configuration.

CIS offers load balancers as a service that you can provision on-demand and then configure to balance loads among a pool of resources, such as VMs.

The current capabilities are:

- Self-service provisioning of load balancers via Horizon or via the OpenStack CLIs or REST APIs.
- Configuring the load balancer with the following parameters:
  - Supported protocols: HTTP (no SSL termination), HTTPS, or custom TCP.
  - Session persistence support.
  - Available load balancing methods: round robin, least connection, or source IP.

Create a Load Balancer

To create a load balancer:

- Create a load balancer pool.
- Assign a Virtual IP (VIP) to the load balancer.
- Add VM members to the Pool.
- Add Health-Check Monitors to the load balancer.
- Attach a Public-Facing Floating IP to the load balancer.
- Test the load balancer.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Create a Load Balancer Pool

A load balancer pool is a logical set of devices, such as web servers, grouped together to receive and process traffic. All requests to the pool first hit the load balancer. The load balancer processes the requests and sends them to the appropriate server in the pool based on the load balancing method that was configured.

1. Create the subnet that's connected to the Internet for the load balancing pool if it doesn't already exist.
2. Click Network > Load Balancers in the Horizon left panel.
3. Click Add Pool, then enter the details for the load balancer pool:
   - Name: A unique name for the load balancer. Use My-Test-LoadBalancer.
   - Provider: The current implementation of load balancing is based on HAProxy. Accept the default.
   - Subnet: The subnet should point to the address space where the VMs/Pools are located. In this example, the VMs that traffic is directed to are located in the private subnet 192.168.3.0/24
   - Protocol: The Load Balancer can accept various types of protocols. You have the ability to choose the type of traffic distribution. In this example use HTTP.
   - Load Balancing Method: Choose the method/algorithm that matches your needs. Use Round-Robin in this example.
4. Click Add.

Assign a Virtual IP Address to the Load Balancer

Assign a Virtual IP address (VIP) to the load balancer. Load balancers listen at this address for incoming requests and route the requests to the appropriate pool members.

1. Click More in the load balancer's Actions column.
2. Click Add VIP.
3. Enter the parameters for the VIP:
   - Name: Enter a name in the Name field, for example "My-Test-VIP".
   - IP address: Specify the private IP address for the VIP on the subnet that the load balancer pool is on. Ensure that the subnet is connected to the Internet.

     Note that this IP address is unreachable. Allocate a floating IP address to this VIP address to make the VIP address reachable/routable for external use.

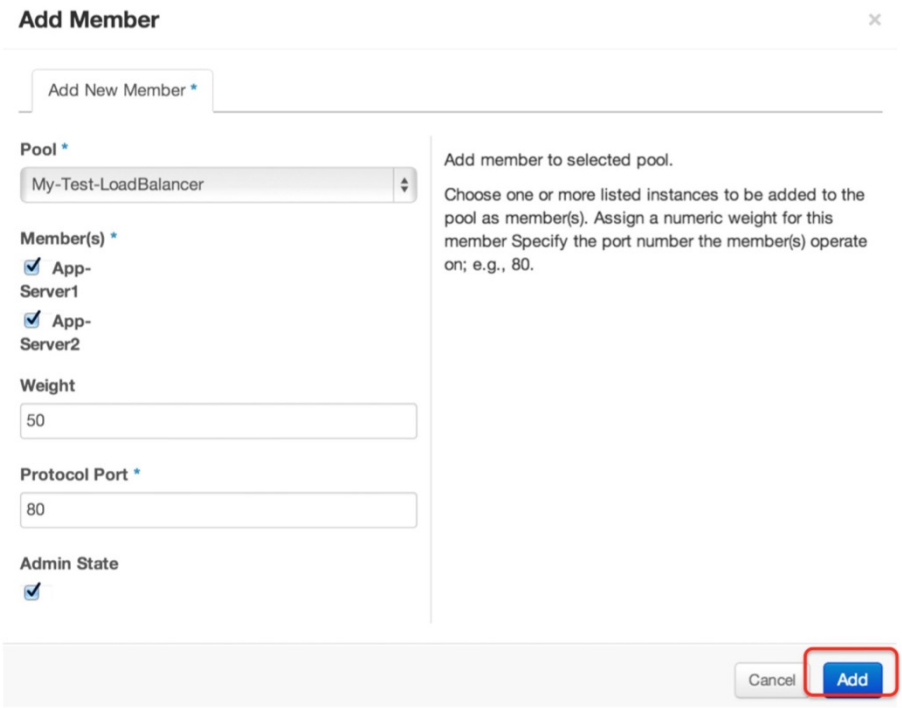
     Notes: Allocating a VIP directly from the floating IP pool is not supported. If you have to use a public address, use an available publicly-accessible IP address. This operation fails if you specify an IP address that is already allocated.
4. Enter the appropriate information in the other fields, then click Add.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Add VM Members to the Pool

To add VM Members to the pool:

1. Click the Members tab.
2. Click Add Member. This adds VMs to the pool to which all the traffic is routed by the load balancer.
3. Provide the following details:
   - Pool: Provide the name of the load balancer pool to which you want to add the members. In this example, you are using the My-Test-LoadBalancer pool that you previously created that points to the private subnet 192.168.3.0/24.
   - Members: The system displays all of the VMs in the pool. Click them. In this example, two VMs, App-Server 1 and App-Server 2, are available in this network as shown. Click their check boxes to add them to the pool. It is assumed that you've created one or more VMs in your project. If not, do so and then return to this step.
   - Weight: Assign a weight to the distribution. This example shows 50, for equal distribution.
   - Protocol Port: Because the VMs in this example are configured as web servers, enter port 80. Or you can enter another port number based on your needs.
4. Click Add to add the members to the pool.



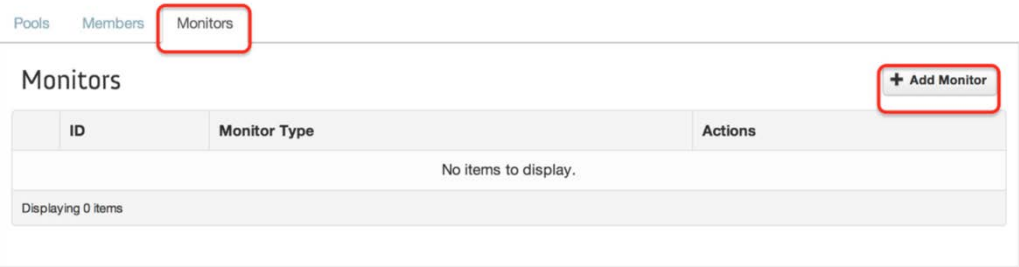
Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Add Health-Check Monitors to the Load Balancer

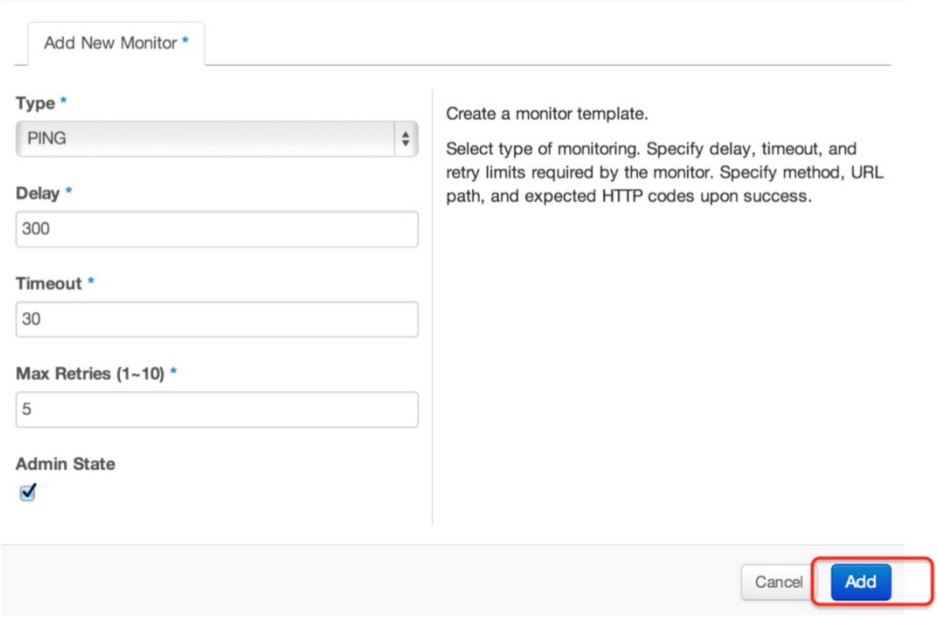
Generally ping isn't the best way to monitor a load balancer. For example, a better way to monitor a web server might be to call a given URL and evaluate the HTTP response code returned. However, for simplicity you will use pings in this example. Refer to Test the Load Balancer on page 32.

To add Health-Check Monitors:

1. Click Monitors.
2. Click Add Monitor.



3. Add monitor details using ping and configure the delay, timeout, and maximum retries.
4. Click Add.



Attach a Floating IP Address to the Load Balancer

The VIP that you created in the private subnet needs a public-facing floating IP address.

To attach a floating IP address:

1. In Horizon click Compute > Access & Security.
2. Click Floating IPs.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

3. Click Allocate IP to Project.
4. Select the floating IP pool, in this case public-floating-601.
5. Click Allocate IP.
6. Click Associate in the Actions column for the floating IP address.
7. In the Manage Floating IP Associations dialog, select the port to be associated. This is the port that was assigned to the load balancer VIP. Select it and click Associate. You will now see the publicly accessible floating IP address for the load balancer.
8. Ping the floating IP address to verify that the load balancer is reachable. If you try to ping the floating IP address and it doesn't work, retry after waiting a minute or two for the floating IP address to be provisioned.

Test the Load Balancer

To test the load balancer, here is a simple test:

1. Start an app server on port 80 (the port that the load balancer is directing HTTP traffic to).
2. Log into the VM:

   $ ssh –i <*path/to/your/local/private/key*> root@<*floating IP address*>
3. Execute vi index.html on the index file for the HTTP server.
4. Add this first line: HTTP/1.0 200 OK Hello from App Server ONE
5. Save the file and exit.
6. Run the HTTP Server: sudo python –m SimpleHTTPServer 80
7. The response should be: Server 1 is listening.
8. Repeat the steps above for Server 2 with the text: HTTP/1.0 200 OK Hello from App Server TWO
9. Now both servers are running.
10. Go to a browser and enter the address of the load balancer. The Load Balancer gets the request and assigns it to App Server 1, which responds with "Hello from App Server One":

When you send the request from the browser for the second time, the load balancer gets the request and assigns it to App Server 2, as it is a Round-Robin assignment. App Server 2 responds with "Hello from AppServer TWO".

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

8. Images and Snapshots

Images

A VM image is a collection of files for a specific operating system that you use to create a server. CIS provides default pre-built images that you access via Launch Instance.

You can create a bootable image by taking a snapshot of an instance from the Horizon Instances screen. These bootable images display in the Images section of the Horizon Images and Snapshots screen. Click Launch for the image from the Images section – the process is the same as launching a new instance from the Instances screen.

You can also import your own images into the Images section and launch them as described above.

Launch a VM from an Existing Image

To launch a new VM using an existing image, refer to Create Your First VM Instance on page 20.

Create an Image

You can create your own image with these formats:

- Iso
- qcow2
- raw
- vdi
- vhd
- vmdk

When building your own image, Windows requires para-virtualized drivers for storage, network, and system devices. Cisco supports Microsoft certified drivers. Drivers for Red Hat are available here.

Note: Cisco recommends that you only use supported drivers.

To create an image:

1. Click **Images & Snapshots** in Horizon.
2. Click **Create Image**.
3. On the **Create an Image** form, type a name for the image.
4. (Optional) Type a description.
5. From the **Image Source** drop-down list, select **Image Location** or **Image File**.
    - If you selected **Image File**, enter the URL for the image.
    - If you selected **Image Location**, browse to the image location.
6. In the **Format** field, select the image format.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Note: Windows images created in VHDX format do not convert correctly to VHD. When you are creating a VHD image, be sure to configure the disk as a static disk, not dynamic.

7. (Optional) Enter the minimum disk usage in gigabytes.
8. (Optional) Enter the minimum RAM usage in gigabytes.
9. (Optional) Select the **Protected** check box to prevent users from deleting this image.
10. Click **Create Image**.

You can now create an instance using this image.

Snapshots

This section describes how to create instance snapshots, volume snapshots, and how to create a volume from a snapshot.

Note: Do not take a snapshot of a snapshot.

Create an Instance Snapshot

When you create an instance snapshot from Horizon you're creating a nova snapshot. Nova snapshots are snapshots of the root disk and do not snapshot any attached volumes or ephemeral storage.

1. Click Instances in the Horizon left panel.
2. In the Actions column, click Create Snapshot for the target instance.
3. In the Create Snapshot dialog, enter a name for the snapshot in the Snapshot Name field.
4. Click Create Snapshot. The snapshot is created and displays in the Horizon Images & Snapshots screen.

Create a Volume Snapshot

In this release, detach the volume from the VM before creating a volume snapshot from Horizon. To avoid having to detach the volume from the VM, you can use the cinder CLI command as discussed below.

To create a snapshot of an in-use volume attached to a running VM:

1. Execute the cinder list command.
2. Pipe the output of the cinder list command through the grep command to discover the ID of each volume attached to the VM.
3. Using the ID of the volume and specifying a name for the snapshot, execute the cinder snapshot-create command to create the snapshot.
4. Example: Create the snapshot "My-First-Snap" for the volume attached to the VM "My-First-VM".

   # cinder list | grep My-First-VM

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

| 242ee41a-fc4e-4e0f-940a | in-use | My-First-VM | 50 | None | true | 3f5a3d7c-55f8-4a21-b352

cinder snapshot-create --force True --display_name My-First-Snap 242ee41a-fc4e-4e0f-940a

Create a Volume from a Snapshot

To create a volume from a snapshot:

1. Click Images & Snapshots in the Horizon left panel.
2. In the Actions column for the source snapshot (image), click Create Volume for the source snapshot.
3. Enter a name for the volume in the Volume Name field.
4. Enter the size for the volume in gigabytes in the Size (GB) field.
5. Click Create Volume.

9. Storage for your VM: Volume and Object

Create Volume Storage and Attach / Mount it to Your VM

Volume storage (also called block storage, sometimes called a physical record) is a sequence of bytes usually containing a number of records. The most common types of block storage are relational database systems like Oracle, MySQL, and DB2. Here you can perform Create, Read, Update, and Delete (CRUD) operations, but unlike object storage, you can modify the content of an individual record.

When you create a VM, normally you will want to add storage to it and the following set of procedures tells you how to do that. You can create a volume out of block storage and attach it to an instance running on CIS. Volumes persist until you delete them (or until you delete a VM to which they are attached), enabling you to control how long you keep your data.

You can attach volume (block) storage to your VMs using Horizon or via the OpenStack CLIs/APIs. For this discussion you will use Horizon.

Create Volume Storage

1. Click Compute > Volumes in the Horizon left panel. You can see a list of other volumes that you have already provisioned if any.
2. Click Create Volume.

   Enter the information needed to create a volume:

   - Name of the volume. For example, **my-first-volume**.
   - Size in GB. Note the amount of available storage displayed in the Volume Limits section on the right side of the dialog.
   - You have the option to choose the volume source. It can be empty, for example for Windows volumes, or you have the option to preload an image.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

- You have the option to choose an availability zone.
- Click Create Volume. This creates a new volume. Now you can attach the volume to a VM.

Attach a Volume to a VM (Linux)

All commands in this section require root privileges as indicated by the # prompt. For the exact command for your system, consult the documentation for your version of Linux.

1. To see the VM's existing devices, log into the instance and execute the following command:

   # fdisk -l

   Note: The parameter in this example is a lower case **L**.

2. Click Compute > Volumes in the Horizon left panel if you are not already in the Volumes screen.
3. From the Volumes table, click More in the target volume's Actions column, then click Edit Attachments.
4. In the Manage Volume Attachments dialog, select the desired instance from the Attach to Instance drop-down.
5. Click Attach Volume.
6. To see the current list of the VM's devices and determine the volume's device name, execute the following command:

   # fdisk -l

   Note: The parameter in this example is a lower case **L**.

7. Format the volume by making the file system:

   WARNING: mkfs erases the contents of the volume. Do NOT execute mkfs if you are mounting a previously used volume whose contents you wish to persist.

   # mkfs -t <*file system type*> /dev/<*device name*>

8. Create a mount point (the directory to read from and write to)

   # mkdir -p /<*mount point*>

9. You can mount the device for one-time use:

   # mount -t <*file system type*> /dev/<*device name*>/<*mount point*>

   Or you can configure the system so the volume will come up every time the VM reboots. Consult the documentation for your version of Linux to see how add this volume to a permanent mount point in /etc/fstab.

Attach a Volume to a VM (Windows)

1. Click Compute > Volumes in Horizon if you are not already in the Volumes screen.
2. From the Volumes table, click More in the target volume's Actions column, then click Edit Attachments.
3. In the Manage Volume Attachments dialog, select the desired instance from the Attach to Instance drop-down.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

4. Click Attach Volume.
5. Click the MM link in the Attached To column for the volume.
6. Click the Console tab. You may have to click the gray bar to invoke the VM.
7. Log into your Windows instance. The volume that you attached will display as a disk in the Windows Disk Manager.
8. Follow the standard procedures for adding a disk to Windows, then create one or more volumes on your new Windows disk.

Detach a Volume from a VM

WARNING: Do **NOT** accidentally detach the volume attached to /dev/vda. This is your root boot disk. If you detach your root boot disk the VM will become inaccessible and all ephemeral data and all data on the root boot disk will be destroyed.

Note: All commands in this section require root privileges as indicated by the # prompt. For the exact command for your system, consult the documentation for your version of Linux.

To detach a volume from a VM:

1. You **MUST** umount the volume.

   WARNING: Before you detach the volume, you **MUST** umount the volume, otherwise you may lose data.

   # umount /<*mount point*>
2. Click Compute > Volumes in the Horizon left panel.
3. Click More in the target volume's Actions column.
4. Click Edit Attachments for the correct volume.

   WARNING: Ensure that you are detaching the correct volume. Do **NOT** detach the root boot disk.
5. Click Detach Volume.

Object Storage

You can create containers and upload and download objects to containers.

Overview

Object storage manages data objects. With objects you can execute Create, Read, Write, and Delete (CRUD) operations, but unlike block storage, you cannot update or modify your objects. To modify or update objects you must completely replace them—in other words, create new versions of them. You create containers and store your objects in containers.

Object store is used most often for unstructured data such as text, images, MRI scans, digital photos, logs files, and media (movies, audio), and is especially used when you want to store huge amounts of information, terabytes and above. So when you view Object storage, think of massively scalable and highly redundant storage.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

OpenStack object storage is ideal for cost-effective, scale-out, distributed storage. It is used to store static data such as virtual machine images, photos, videos, email storage, backups and archives.

Object storage works via containers and objects. A container is a storage compartment used to organize data. For example, you might create a Movie container to store all your movies. Objects are basic units of storage for object storage.

You can create containers, set permissions on them (also known as Access Control Lists or ACL), and upload and download objects via Horizon or the OpenStack CLIs/APIs.

The data in object storage consists of a location (container), the object's name, and any metadata consisting of key/value pairs.

Create a Container

To create a container:

1. Click Object Store > Containers in the Horizon left panel.
2. Click Create Container.
3. Enter a container name in the Container Name field.
4. The Container Access default is Private.

   WARNING: If you change the default to Public anyone with the public URL can gain access to the objects in the container.
5. Click Create Container.

Upload an Object to a Container

1. Click the Containers tab in the Horizon left panel.
2. Click the name of the target container.
3. Click Upload Object.
4. Enter a name for the object in the Object Name field.
5. Click Browse to locate a file to upload to the container.
6. Select the file.
7. Click Open.
8. Click Upload Object. The object name appears next to the container the object was uploaded to.

Delete an Object

To delete an object:

1. Navigate to Object Store > Containers in the Horizon left panel.
2. Click the object check box. To delete multiple objects select multiple object check boxes.
3. Click Delete Objects.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Delete a Container

NOTE: Before attempting to delete a container make sure that the container is empty.

To delete a container:

1. Navigate to Object Store > Containers in the Horizon left panel.
2. Click the container More button.
3. Click Delete Container.

10. Accessing CIS via OpenStack CLIs & REST APIs

You can access CIS using Open Stack CLIs. OpenStack APIs are available but some are not supported (Ceilometer, Autoscaling, Availability Zones, and VPN-as-a-Service).

Generate Your API Key

1. Click the down arrow to the right of your login email address in the menu bar.
2. Click Settings > Generate API Key.
3. Note the API key that appears.
4. Use the API key as your OpenStack API password environment variable (OS_PASSWORD) when making OpenStack CLI/API calls.
5. Use your login (your email address) for your OpenStack API username environment variable (OS_USERNAME) when making OpenStack CLI/API calls.
6. If you click Regenerate API Key, you will need to update all of your OpenStack CLI/API scripts with your new OS_PASSWORD environment variable.

Download the OpenStack RC file

You'll need to know the appropriate environment variables to access the OpenStack CLI, and you'll need a list of your project's OpenStack REST API endpoints to access the API.

Note: Use your login email address for your API username environment variable and use your API key for your API password environment variable as discussed in Generate Your API Key on page 39. The API key is not the same as the password that you use when you log into the system.

1. In Horizon click Compute > Access & Security > API Access.
2. Click Download OpenStack RC File for the environment variables that you'll need to use the OpenStack CLI.
3. You see a table with a list of your project OpenStack REST API endpoints in the API Access screen.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

11. Glossary

Term	Definition
API	Application Programming Interface. A set of programming instructions and standards for accessing a web-based software application. OpenStack has a number of APIs for creating Instances, Images, Authentication, etc.
Block Storage	A sequence of bytes (usually a whole number of records) having a maximum length called a block size. Used in database management systems such as Oracle. Block storage is typically mounted as a drive.
Cinder	An OpenStack Block Storage service that maintains block devices that can be attached to virtual machine instances.
Cisco Intercloud Services	The Cisco Cloud Infrastructure as a Service (IaaS) that contains OpenStack plus many additional services.
Cisco Intercloud Services Console	The **Projects** page on which you create and manage your CIS projects and instances and from which you can launch instances, view instances, view data center system status, and access Horizon.
Cisco Intercloud Services Portal	The initial point of entry into CIS (https://cloud.cisco.com).
CLI	OpenStack Command Line Interface. Provides users with a series of commands and arguments so they can interact with OpenStack. For example, you can create an instance or volume, create a snapshot, attach a volume, etc.
Data Center	Houses critical component resources (computers, storage, networks) in a controlled environment under centralized management that enables enterprises to operate around the clock according their business needs.
Ephemeral Storage	Ephemeral storage, also known as an ephemeral disk, is like a temporary scratch pad that the systems reads from and writes to. It is non-persistent storage that is automatically created when a VM is created and destroyed when a VM is terminated and the ephemeral data is not saved.
Flavor	Defines the CPU type, RAM, and the amount of storage for an instance.
Gateway	You connect a router to an external URL via a gateway.
Floating IP Address	In CIS a floating IP address is a public IP address (reachable from the Internet) that can be allocated to a project from a pool of public IP addresses and then associated with a network resource in the project like a VM.
Horizon	The OpenStack Horizon graphical user interface that is used for creating instances, virtual volumes, and virtual network components, etc. and managing your projects. Also known as the Horizon Dashboard.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Image	Refer to snapshot.
Instance	Same as virtual machine (VM) or VM instance. Also called a server.
Instance Type	Same as flavor.
Key pair	Used for authentication of your instances. Each key has two parts, public and private. You use **Create Keypair** to generate public and private keys. The public key is maintained and supplied by OpenStack. You can use the Horizon Console to generate a key pair.
Load Balancer	Distributes inbound network traffic across multiple VMs or other network resources to optimize resources and throughput to lessen the likelihood that a single network resource will be overwhelmed.
Nova	An OpenStack Compute service that controls cloud computing fabric, virtualization, CPU, RAM, NICs, and hard drives.
Object Storage	Collection of digital content such as photos, MRI scans, videos, etc. Provides eventually consistent and redundant storage as well as retrieval of fixed digital content. Differs from block storage because with object storage you have no update ability—you can insert and retrieve an object but you cannot modify it.
OpenStack	The open source infrastructure as a service (IaaS) software used by Cisco to create CIS.
Project	A virtual workspace in the Cisco cloud in which users can create VM, networks, routers, load balancers, etc.
Red Hat Enterprise RHEL	The default operating system used by VMs created using CIS.
Security Group	A set of network traffic filtering rules applied to an instance.
Snapshot	A point-by-point copy of an OpenStack storage volume or image. You can use snapshots to back up volumes. You can use image snapshots to back up data, gold images or additional servers.
Tenant	The entity that owns a project is called a **tenant**. A tenant can have more than one project.
VIP	Virtual IP address. This is an available unused private IP address that can be assigned to a network resource in a project like a load balancer. The VIP is then associated with a floating IP address so the network resource can communicate with the Internet.
Virtual Compute	The section of Horizon from which you can create and manage instances, volumes, images, snapshots, and access and security.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Virtual Machine (VM)	A VM (also called an instance or a server) is created by a user and is composed of a guest operating system (an image), a CPU, storage, and network components.
Virtual Network	The portion of the Cisco cloud that creates the virtual network components.
Virtual Storage	The portion of the Cisco cloud that creates storage (volumes).
Volume Storage	Persistent block storage devices that may be attached and unattached from instances but only attached to one instance at a time.
VPN	Virtual Private Network.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

12. Appendix: Resource Segregation

Filters are used for scheduling VM instances. When the filter scheduler receives a request for a resource, it applies filters to determine which hosts are eligible for consideration when dispatching a resource.

Creating a Filter Policy

You need to explicitly create a new server group and associate the group with the new affinity/anti-affinity filter policy. You can create a server group using the command-line client or REST API.

Use the Nova Command-Line Tool

Create a server group using the following command syntax:

```
nova server-group-create < group_name > [< policy >]
```

where

- **group name** is the name of the server group.
- **policy** indicates the rules used by the server group, for example, affinity or anti-affinity.

For example:

```
nova server-group-create AF1 anti-affinity
```

Use the REST API

Create a server group by sending a POST message:

```
POST /v2/< tenant_id >/os-server-groups
```

The message in JSON format:

```
{
    "server_group": {
        "name": "< group_name >",
        "policies": ["< policy >"]
    }
}
```

where

- **group name** is the name of the server group.
- **policy** indicates the rules used by the server group, for example, affinity or anti-affinity.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Placing Instance on Different Computer Hosts

To use the GroupAntiAffinityFilter capability, specify a group name with the **--hint group** parameter when booting the instances. As long as you use the same --hint group parameter, the Nova Scheduler places each instance on a different compute host.

Use the Nova Command-Line Tool

Deploy an instance using the following command syntax:

```
$ nova boot <name> --nic [net-id=<private-net-uuid> --flavor <flavor> \
--image <image> --hint group=<anti-affinity-policy>
```

For example:

```
$ nova boot server-01 --nic net-id516783fc-2170-47f1-ba8d-a4b39a839d51 \
--flavor GP-Small --image centos-6.5_x86_64-2014-06-04-v3 \
--hint group=anti-affinity
```

Use the REST API

Deploy an instance by sending a POST message:

```
POST /v2/< tenant_id >/os-server-groups
```

The message in JSON format:

```
{
    "server_group": {
        "name": "< group_name >",
        "imageRef": "<image-id>",
        "flavorRef": "<flavor-id>",
        "os:scheduler_hints":{"group":" anti-affinity-policy "}
    }
}
```

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

13. Appendix: CIS Instance Customization

CIS VM instance customization occurs through standard Openstack cloud platform mechanisms by way of a metadata service and a process that runs at startup when new VM instances are booted. The metadata service is a Nova component function that serves as a data source for VM instance data. The default metadata source in use on CIS platform is a network based service that runs on the Nova API endpoints. The system program that consumes the data is referred to as **cloud-init**.

Cloud-init and Cloudbase-init

Cloud-init ships by default on all modern Linux operating systems. It is enabled by default to run at boot-up of an instance and consume parameters from various data sources, either local disk or network-based metadata service. For Windows operating systems, a third-party product known as **cloudbase-init** can be added to Windows guest instances to allow it to consume this VM instance data. All CIS public Windows images ship with **cloudbase-init** installed.

Typically, a normal VM boot process leverages the metadata service and **cloud-init** processes for injecting SSH keys and VM name parameters into the instance operating system as user data. However, you can insert a number of other customizations or scripts to be executed by **cloud-init** by passing in additional user data either via the Horizon launch instance wizard, or via the CLI and API. The most common formats of user data are shell scripts (**#!/bin/bash**) or cloud-config (**#cloud-config**). **Cloud-init** scripts run late in the boot sequence so you can run any type of customization or software installation process for which you can write a script. The **#cloud-config** option supports a YAML-based format that allows you to configure a wide array of options including additional SSH-keys, custom run commands, puppet recipes, or some other system level configurations.

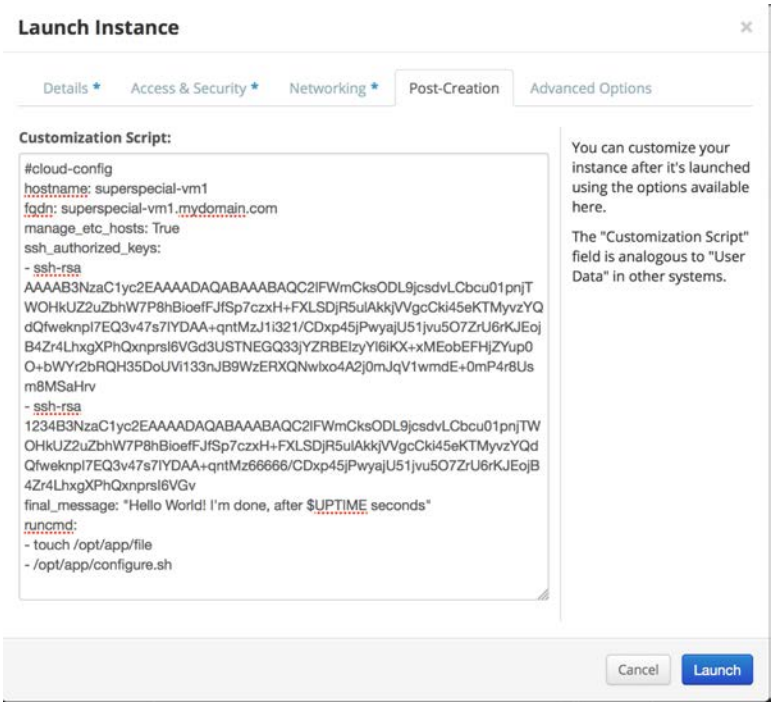
You can find a comprehensive list of **#cloud-config** options at this site: http://cloudinit.readthedocs.org/en/latest/topics/examples.html.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Sample Customization Options

Sample 1

From the Horizon dashboard, the **Post-Creation** tab has a **Customization Script** field that allows you to insert user data for **cloud-init** to process at VM start-up. The following example uses **#cloud-config** to configure a fully qualified domain name for the system and inject multiple SSH authorized keys, then shows how to run commands for configuring an application:



From the CLI, you can insert custom data by passing the **–user-data** option to the Nova boot command:

nova boot --flavor GP2-Medium --nic net-id=4c3bd6e9-fc80-4988-b415-f829f3cba47c --image RHEL7 --user-data ./userdata.txt superspecial-vm1

where **./userdata.txt** contains the shell script or cloud config data you want executed.

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.

Sample 2

This example, from cloud-config-puppet.txt, has the instance contact a specific puppet master at boot for further processing:

```
#cloud-config
puppet:
 conf:
  agent:
    server: "puppetmaster.example.org"
  ca_cert: |
    -----BEGIN CERTIFICATE-----
    MIICCTCCAXKgAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDDAJjYTAe
    Fw0xMDAyMTUxNzI5MjFaFw0xNTAyMTQxNzI5MjFaMA0xCzAJBgNVBAMMAmNhMIGf
    MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCu7Q40sm47/E1Pf+r8AYb/V/FWGPgc
    b014OmNoX7dgCxTDvps/h8Vw555PdAFsW5+QhsGr31IJNI3kSYprFQcYf7A8tNWu
    1MASW2CfaEiOEi9F1R3R4Qlz4ix+iNoHiUDTjazw/tZwEdxaQXQVLwgTGRwVa+aA
    qbutJKi93MILLwIDAQABo3kwdzA4BglghkgBhvhCAQ0EKxYpUHVwcGV0IFJ1Ynkv
    T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwDwYDVR0TAQH/BAUwAwEB/zAd
    BgNVHQ4EFgQUu4+jHB+GYE5Vxo+ol1OAhevspjAwCwYDVR0PBAQDAgEGMA0GCSqG
    SIb3DQEBBQUAA4GBAH/rxlUIjwNb3n7TXJcDJ6MMHUlwjr03BDJXKb34Ulndkpaf
    +GAlzPXWa7bO908M9I8RnPfvtKnteLbvgTK+h+zX1XCty+S2EQWk29i2AdoqOTxb
    hppiGMp0tT5Havu4aceCXiy2crVcudj3NFciy8X66SoECemW9UYDCb9T5D0d
    -----END CERTIFICATE-----
```

Copyright 2014 - 2015 Cisco Systems, Inc. All rights reserved.